VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT

INSTITUT OF INFORMATICS

APLIKACE NOVÝCH METOD PRO ZABEZPEČENÍ VZDÁLENÝCH POČÍTAČŮ

USE OF NEW METHODS FOR SECURING REMOTE COMPUTERS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR
VLADIMÍR ŠANDERA

VEDOUCÍ PRÁCE
SUPERVISOR
ING. VIKTOR ONDRÁK, PH.D.

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Šandera Vladimír

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a
zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Aplikace nových metod pro zabezpečení vzdálených počítačů

v anglickém jazyce:

Use of New Methods for Securing Remote Computers

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. USA : McGraw-Hill, 2010. 377 s. ISBN 978-0-07-159118-8
AYCOCK J. *Computer Viruses and Malware*. USA : Springer, 2010. 227 s. ISBN 978-0-387-3036-2
SZÖR P. *The Art of Computer Virus Research and Defense*. USA : Addison Wesley Professional, 2005. 744 s. ISBN 0-321-30454-3
JANOUCH V. *Internetový marketing Prosaďte se na webu a sociálních sítích.* 1. vydání. Brno : Computer Press, a.s., 2010. 304 s. ISBN 978-80-251-2795-7

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/2011.

L.S.

Ing. Jiří Kříž, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 25.05.2011

Abstrakt

Tato práce se zabývá zabezpečením počítačů pro domácnosti a malé firmy. Nejdříve analyzuji současný stav, jak zabezpečení počítačů probíhá. V teoretické části budu popisovat typy počítačových infekcí, které se dnes vyskytují a používané techniky pro odstranění těchto infekcí. Analyzuji současný stav na trhu technické podpory pro koncové uživatele a popisuji svoji podnikatelskou činnost. V návrhu řešení představuji novou metodu zabezpečení počítačů na dálku a výhody, které tento nový koncept přináší. Zaměřuji se také na ekonomické přínosy využití modelu poskytování technické podpory na dálku, jako je snížení výdajů, centralizace a zvýšení efektivity.

Abstract

This paper is focused on computer security services for households and small businesses. First I analyze the current situation on the computer security market. In theoretical part of the paper I will describe known types of security threats as viruses, malware, rootkits and counter measures against these threats. In practical part of the paper I analyze current conditions on the market, my business project and I introduce new concept for securing remote computers. I will talk about economical advantages of this concept as cost reduction, centralization of resources and increase in efficiency.

Klíčová slova

Zabezpečení počítačů, odvirování, virus, malware, rootkit, antivirus, technická podpora, připojení na dálku, LogMeIn

Keywords

Computer security, virus removal, virus, malware, rootkit, antivirus, technical support, remote connection, LogMeIn

Bibliografická citace

ŠANDERA, V. *Aplikace nových metod pro zabezpečení vzdálených počítačů.* Brno : Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 57 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph. D.

Čestné prohlášení:

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 25. května 2011

.....

Vladimír Šandera

Poděkování

Děkuji vedoucímu mé bakalářské práce panu Ing. Viktoru Ondrákovi, Ph.D., za cenné rady, konzultace a připomínky, které mi poskytoval při zpracování mé bakalářské práce.

Obsah

1. Úvod 10
2. Vymezení problému a cíle práce 11
3. Analýza současného stavu 12
3.1 Analýza podnikatelské činnosti 12
3.1.1 Základní informace 12
3.1.2 Nabízené služby 12
3.1.2.1 Hlavní služba 12
3.1.2.2 Doplňkové služby 13
3.1.3 Analýza marketingu 13
3.1.4 Současné finanční výsledky 14
3.2 Průzkum stávajících zákazníků 17
3.2.1 Antivirové produkty 17
3.2.2 Technické problémy 18
3.2.3 Nedostatky nabízených služeb 19
3.3 Analýza trhu 19
3.3.1 Zhodnocení trhu 19
3.3.2 Konkurence 21
3.3.2.1 Antivirové společnosti 21
3.3.2.2 Nezávislé PC servisy 22
3.3.3 Nedostatky nabízených služeb 22
3.3.3.1 Omezená geografická dostupnost 22
3.3.3.2 Nízká efektivita 23
3.3.3.3 Dlouhá reakční doba 23
3.4 Shrnutí analýzy 23
4. Teoretická východiska řešení 25
4.1 Typy počítačových infekcí 25
4.1.1 Malware 25
4.1.1.1 Virus 25
4.1.1.2 Červ 26
4.1.1.3 Zadní vrátka (backdoor) 26
4.1.1.4 Trojský kůň 26
4.1.1.5 Spyware 27
4.1.1.6 Adware 28
4.1.1.7 Logická bomba 28

4.1.2 Rootkity 29
4.1.2.1 User-mode rootkit 30
4.1.2.2 Kernel-mode rootkit 31
4.1.2.3 Virtuální rootkit 33
4.1.2.4 Budoucnost rootkitů 35
4.2 Metody prevence a zabezpečení 36
4.2.1 Detekce malware 37
4.2.1.1 Statická detekce 37
4.2.1.2 Dynamická detekce 39
4.2.2 Detekce rootkitů 40
4.2.2.1 MS Windows anti-rootkit techniky 40
4.2.2.2 Software-based detekce 41
4.2.2.3 Hardware-based detekce 42
4.2.2.4 Detekce virtuálních rootkitů 43
5. Návrh řešení 44
5.1 Model poskytování služeb online 44
5.2 Výhody online modelu 44
5.2.1 Pokrytí většího trhu 45
5.2.2 Zvýšení efektivity 45
5.2.3 Snížení reakční doby 46
5.2.4 Snížení výdajů 46
5.2.5 Efektivnější řízení 46
5.3 Realizace přechodu na online model 46
5.3.1 Zakoupení aplikace pro vzdálené připojení 47
5.3.2 Úprava webových stránek 48
5.3.3 Úprava marketingových kampaní 50
5.4 Podnikatelská strategie a cíle 51
5.4.1 Rozšíření služeb 51
5.4.2 Vytvoření pracovního teamu 51
5.5 SWOT analýza 52
6. Zhodnocení a závěr 54
Seznam použité literatury 55
Knižní publikace 55
Internetové zdroje 55
Seznam obrázků 57
Seznam grafů 57

1. Úvod

V této práci popisuji, jak vypadá trh zabezpečení počítačů v České republice. Nejdříve se věnuji popisu jednotlivých typů počítačových infekcí. Poté analyzuji současný stav trhu, jeho segmenty a jaké jsou nedostatky v oblasti technické podpory a zabezpečení PC koncových uživatelů. Na základě této analýzy poté představím nový koncept zabezpečení počítačů a predikci, jakým směrem se bude tento trh vyvíjet do budoucna.

Ochrana proti počítačovým infekcím a zabezpečení počítače postihuje všechny uživatele počítačových systémů. Největší investice do zabezpečení počítačů a sítí se vynakládají ve firmách, které ve většině případů mají dostatečné finanční prostředky pro najmutí IT odborníků či přímo zřízení celého IT oddělení, které se zabývá zabezpečením firemních dat.

Jiná je situace v sektoru domácích uživatelů, živnostníků a malých firem. Koncoví uživatelé a malé společnosti nemají dostatečné finanční prostředky na najmutí IT odborníků a spoléhají na komerční antivirové aplikace, které jsou k dispozici zdarma nebo za přijatelný roční poplatek.

Z důvodu nízké úrovně zabezpečení a nízké technické gramotnosti v sektoru domácích uživatelů jsem zahájil podnikatelskou činnost zaměřenou na zabezpečení výpočetní techniky v tomto segmentu. V této práci se zaměřuji primárně na analýzu mojí činnosti a trhu, na kterém působím. Na základě analýzy jsem sestavil návrh na zlepšení služeb na trhu, který aplikuji na mé podnikatelské aktivity.

2. Vymezení problému a cíle práce

Vymezení problému

Nedostatečné pokrytí trhu zabezpečení počítačů v segmentu koncových uživatelů. Nedostatečné množství firem poskytujících nezávislou technickou podporu v oblasti zabezpečení počítačů domácím uživatelům. Služby zabezpečení, které jsou k dispozici, nejsou standardizované a mají velké množství nedostatků.

Cíl práce

Cílem této práce je navrhnout nový koncept zabezpečení počítače a poskytování služeb technické podpory pro koncové zákazníky. Pomocí nového modelu poskytování technické podpory a využitím nových technologií na trhu se snažím dosáhnout vyšší kvality a dostupnosti služeb v oblasti zabezpečení počítačů pro koncové uživatele.

3. Analýza současného stavu

V této části práce popisuji současnou situaci na trhu zabezpečení počítačů. Nejdříve se věnuji popisu mé podnikatelské činnosti v oblasti zabezpečení počítačů a poté analyzuji současnou situaci na trhu v segmentu koncových uživatelů.

3.1 Analýza podnikatelské činnosti

3.1.1 Základní informace

V březnu 2010 jsem zahájil svoji činnost jako OSVČ v oblasti počítačové bezpečnosti a spustil jsem projekt "Odvirování PC". Cílem mého projektu je poskytovat technickou podporu v oblasti zabezpečení PC. Moje služby jsou zaměřeny na koncové uživatele ICT a segment malých firem (právnické i fyzické osoby). Podnikatelskou činnost provozuji v oblasti města Brna a jeho okolí.

Momentálně pracuji sám. Množství zákazníků využívající mých služeb se aktuálně pohybuje v rozmezí 10 až 15 měsíčně. Projekt v této chvíli financuji z vlastních zdrojů, moje investice směřuji primárně na reklamní kampaň a na správu, design a SEO optimalizaci webových stránek.

3.1.2 Nabízené služby

3.1.2.1 Hlavní služba

Základní službou mého podnikání je Odvirování PC. Dostupnost služby je v okresech Brno-město a Brno-venkov. Reakční doba služby se pohybuje v řádu hodin. Tato služba tvoří hlavní zdroj mých příjmů. Odvirování PC je nabízeno za fixní cenu 500 Kč. Jedná se o jednorázovou službu.

3.1.2.2 Doplňkové služby

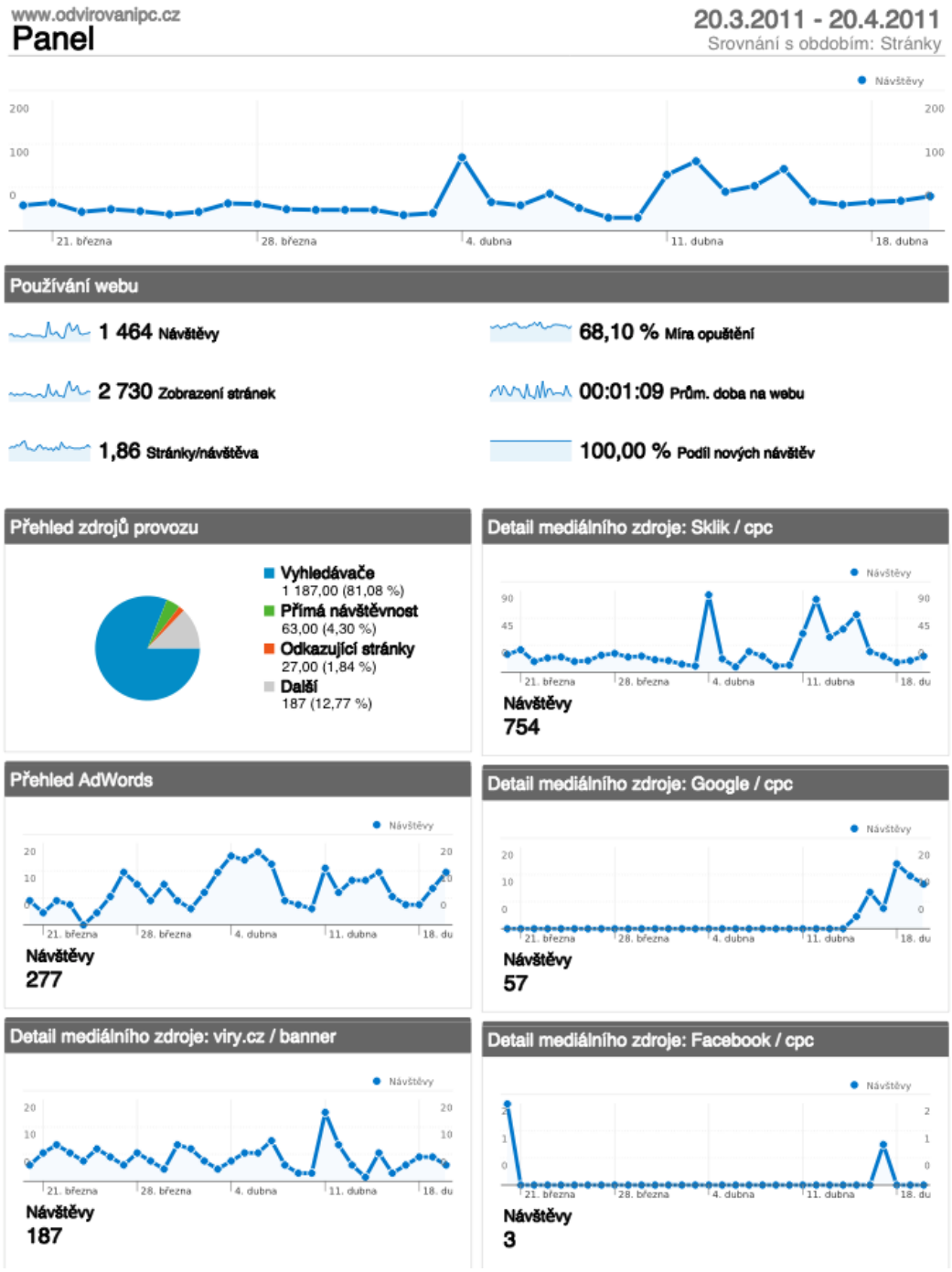
K základní službě Odvirování PC jsem po několika měsících přidružil i další doplňkové služby Instalace Antivirového Programu a Zrychlení PC. Tyto služby nabízím dle vlastního uvážení zákazníkům jako doplněk k základní službě, aby byl můj servis více komplexní. Doplňkové služby jsou zpoplatněny poplatkem 300 Kč, takže zároveň slouží jako diverzifikace příjmů.

3.1.3 Analýza marketingu

Nejdříve jsem zákazníky oslovoval formou inzerátů, které jsem umístil na různé internetové servery. Tuto formu reklamy mi pomáhal realizovat můj partner Ondřej Konečný, který provozuje službu Vkládání Inzerátů (www.vkladani-inzeratu.cz). Přes jeho službu jsem každý měsíc vkládal inzeráty na 70 inzertních serverů. Dále jsem zpravoval a zabezpečoval počítače rodině a známým, kteří rozšířili kladnou referenci o mých službách a pomohli mi získat další zákazníky z řad jejich známých a přátel.

V květnu 2010 jsem spustil vlastní internetové stránky www.odvirovanipc.cz , které nyní slouží jako můj hlavní kanál pro získávání nových zákazníků. Několik týdnů po zprovoznění internetových stránek jsem spustil reklamní kampaň na portálu Seznam.cz, přes jeho reklamní systém Sklik. Systém Sklik je momentálně můj nejaktivnější reklamní kanál, generující měsíčně přibližně 1 000 unikátních přístupů na můj web. Dále provozuji reklamu ve vyhledávači Google, přes jeho reklamní systém AdWords a mám také banner na Českém serveru www.viry.cz, který se zabývá problematikou počítačové bezpečnosti. Celkový počet přístupů na můj web se pohybuje kolem 1500 unikátních návštěvníků měsíčně.

Zde je rozpis statistik přístupů na webové stránky www.odvirovanipc.cz za období 20.3. 2011 - 20.4. 2011. Za toto období web zaznamenal 1464 unikátních přístupů. 74% těchto přístupů pocházelo z PPC reklamy.



Obr. 1: Návštěvnost webu, zdroj: z vlastních dat generováno https://www.google.com/analytics

3.1.4 Současné finanční výsledky

Zde uvádím ekonomická data projektu za celou dobu jeho fungování, tj. od března 2010. Celková doba fungování projektu je v této chvíli 14 měsíců.

Počet zákazníků	143
Výdaje celkem	47 654 Kč
Fixní výdaje	9 628 Kč
Variabilní výdaje	38 026 Kč
Var. výdaje na zákazníka	266 Kč
Příjmy celkem	63 635 Kč
Příjmy na zákazníka	445 Kč
Zisk celkem	15 981 Kč
ROI	134 %

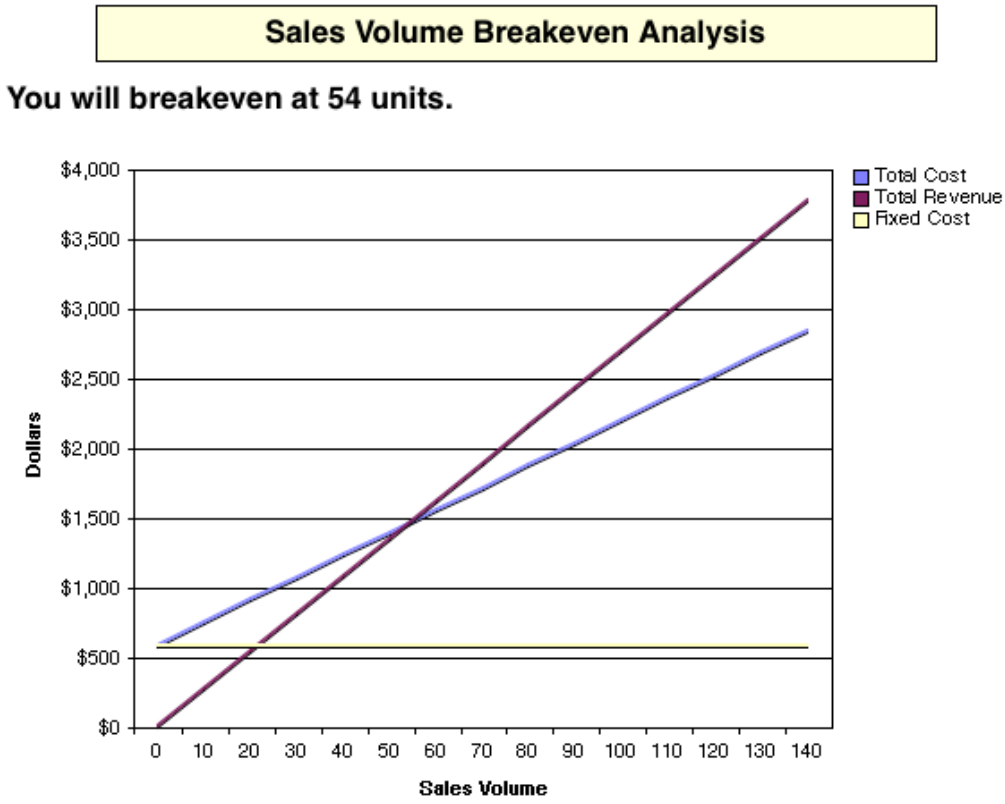
Zde uvádím rozpis daňové povinnosti a zdravotního pojištění za rok 2010. Vzhledem k tomu, že mám status studenta, neplatím sociální pojištění.

Daňová povinnost	
Zaokrouhlený základ daně:	15 900,00 Kč
Daň před slevami:	**2 385,00 Kč**
• základní sleva na poplatníka:	24 840,00 Kč
• student :	4 020,00 Kč
Daň po uplatnění slev:	**0,00 Kč**
Daňový bonus :	0,00 Kč
Doplatek"+" (přeplatek"-") daně:	**0,00 Kč**

Zdravotní pojištění	
Vyměřovací základ ZP :	7 990,50 Kč
Zdravotní pojištění :	1 079,00 Kč
Zaplacené zálohy na ZP :	0,00 Kč
Doplatek zdravotního pojištění:	1 079,00 Kč

Obr. 2: Daňová povinnost a zdravotní poj., zdroj: z vlastních dat generováno http://www.podnikatel.cz

Zde přikládám graf vygenerovaný na základě uvedených čísel. Graf byl vygenerován v rozhraní amerických stránek, takže uvedené částky bylo třeba převést z Kč na USD. Částky jsem převedl na USD podle aktuálního kurzu ke dni 25. duben (1 USD = 16,518 Kč). Z grafu můžeme vidět, že bodu zvratu bylo dosaženo při 54. zákazníkovi a projekt již generuje zisk.



Your breakeven point is where your profit equals zero. As long as your gross margin is greater than zero, every unit sold after you have reached your breakeven point will add to your profitability. If your gross margin is less than zero, regardless of the units sold, there is no breakeven point.

Breakeven Analysis Summary	
Variable Cost	**$16.10 per unit**
Fixed Cost	$583.00
Expected Sales	143 units
Price	$26.94 per unit
Total Revenue	**$3,852.42**
Total Variable Costs	**$2,302.30**
Profit	**$967.12**

Obr. 3: Analýza bodu zvratu, zdroj: z vlastních dat generováno http://www.calculatorplus.com

Podrobný rozpis výdajů:

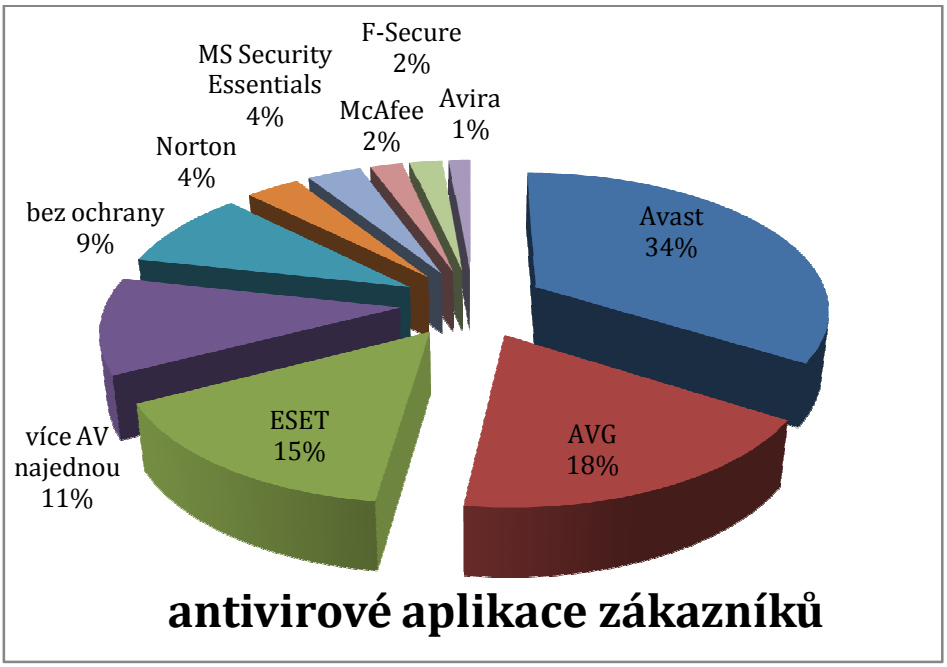
webhosting + domény	3 528 Kč
tvorba webu	4 210 Kč
SEO	750 Kč
Software pro vzdálené připojení	6 100 Kč
Zopim chat	364 Kč
Sklik reklama	15 000 Kč
AdWords reklama	8 000 Kč
banner na www.viry.cz	3 660 Kč
účty za telefon (T-Mobile)	5 500 Kč
Skype	542 Kč

Podnikání provozuji ze svého trvalého bydliště a využívám k němu svůj osobní počítač, do výdajů tedy nezapočítávám cenu nájmu a energií nebo výdaje na výpočetní techniku. Do fixních výdajů jsem zařadil webhosting + domény a software pro vzdálené připojení. Výdaje na telefonní hovory nebylo možné přesně určit, takže jsem je stanovil odhadem. Ostatní výdaje jsem sestavil podle archivovaných faktur.

3.2 Průzkum stávajících zákazníků

3.2.1 Antivirové produkty

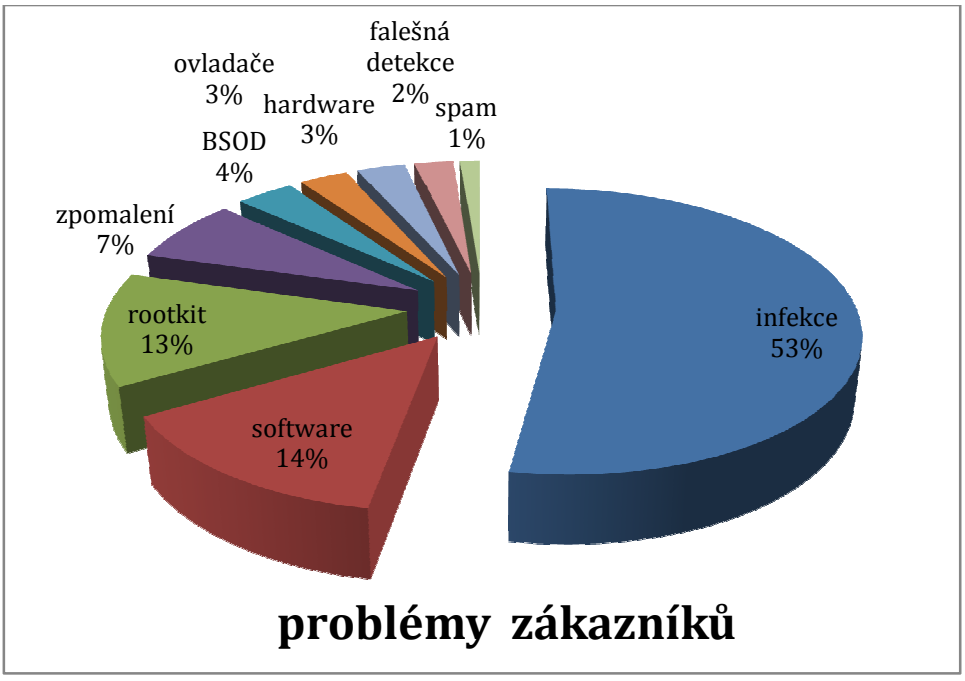
Buduji svoji vlastní interní databázi, kde si u každého zákazníka ukládám informace o tom, jaký používá antivirový produkt. Statistika používaných antivirových aplikací je vidět v následujícím grafu.



Graf 1: Antivirové aplikace zákazníků, zdroj: vlastní

3.2.2 Technické problémy

Zpracovávám interně také data o technických problémech obsloužených zákazníků. Tyto informace slouží k analýze potřeb zákazníků a pro úpravu nabídky služeb.



Graf 2: Problémy zákazníků, zdroj: vlastní

3.2.3 Nedostatky nabízených služeb

Provedl jsem u zákazníků průzkum nedostatků mých služeb. Tímto způsobem jsem získal náměty na zlepšení. Zákazníci nejčastěji uváděli u mých služeb následující 3 negativa:

a) Dlouhá reakční doba: V případě, že se zákazníkovi zaviruje počítač, musí můj příjezd a provedení servisního zásahu čekat, někdy i několik hodin. Většina zákazníků vyžaduje příjezd v co nejkratším možném čase.

b) Nízká informovanost o délce zásahu: Zákazníci chtějí být dopředu informováni o délce odvirování počítače, aby si mohli naplánovat další činnosti v průběhu dne.

c) Nedostatečný rozsah nabízených služeb: Velké procento zákazníků nemá ve skutečnosti problém s infekcí, ale jedná se o problém s operačním systémem či jiný softwarový problém. Zákazník často nedokáže diferencovat mezi infekcí a jiným technickým problémem na počítači. Chybějící služby v oblasti MS Windows troubleshooting a dalších softwarových aplikací.

3.3 Analýza trhu

V následujících kapitolách budu analyzovat tržní okolí firmy. Zaměřím se hlavně na analýze potenciálních zákazníků, konkurence a služeb.

3.3.1 Zhodnocení trhu

Segment středních a velkých firem je orientován převážně na komplexní systém služeb velkých dodavatelů bezpečnostních řešení, není tedy v mých silách do tohoto segment proniknout. V analýze se tedy zaměřím na segment malých firem (právnických I fyzických osob) a občanů.

Podle posledních údajů Ministerstva vnitra je v oblasti mého zájmu (okresy Brno-město, Brno-venkov) 118 129 domácností. „56,6% české populace je každodenními uživateli internetu“[1]. Velikost trhu tedy je 66 152 potencionálních zákazníků.

Na obrázku č. 4 můžeme vidět, že počet uživatelů internetu, kteří jej používají každý den, vzrostl od roku 2005 do roku 2010 z 29,7 % na 56,6 %, což je téměř dvojnásobný nárůst.

Jednotlivci, kteří použili internet v posledních 3 měsících každý nebo skoro každý den

	2005			2010		
	v tisících *thousand*	%[1)]	%[2)]	v tisících *thousand*	%[1)]	%[2)]
Celkem	829.0	9.5	29.7	3,090.4	35.0	56.6
Věková skupina						
16–24	240.1	17.6	27.7	825.7	69.2	75.0
25–34	232.9	13.6	33.6	862.5	51.9	62.4
35–44	171.7	12.7	30.8	635.3	40.8	51.2
45–54	124.2	8.4	28.6	433.9	31.6	48.1
55–64	54.5	4.1	26.6	250.6	16.9	40.1
65–74	.	.	.	64.6	7.1	37.3
75+	.	.	.	17.8	2.7	54.0

Obr. 4: Uživatelé s každodenním využitím internetu[1]

Chování ve vztahu k informační bezpečnosti v cílovém zákaznickém segmentu se dá charakterizovat takto:

- nízká povědomost o bezpečnostních rizicích
- nízká ICT odbornost
- snaha o co největší úspory při nákupu antivirových programů, firewallů

[1] ČSÚ. *Využívání ICT jednotlivci.* 2010. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/vyuzivani_ict_jednotlivci_2005_2010/$File/Vyu%C5%BE%C3%ADv%C3%A1n%C3%AD_ICT_jednotlivci_2005_2010.xls

- stále častější využití internetu pro činnosti vyžadující citlivá data jako je přístup k bankovnímu účtu a nákup zboží

Z obrázků č. 5 a č. 6 můžeme vidět, že i přes silný nárůst využití internetu pro nakupování se příliš nezvyšuje počítačová vzdělanost a technické dovednosti uživatelů.

PC dovednosti : Instalace nových software aplikací				
	celkem (16–74 let) *total (16–74)*			
	% z celku *% total*		% z uživatelů počítače *% of PC users*	
	2006	2009	2006	2009
Česká republika	20.4	27.1	33.7	37.8

Obr. 5: PC dovednosti uživatelů, zdroj: ČSÚ. *Počítačové dovednosti.* 2010. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/pocitacove_dovednosti/$File/3_pc_dovednosti_eu.xls

Koncoví PC uživatelé : Nákupy přes internet pro soukromé účely				
	celkem (16–74 let) *total (16–74)*			
	% z celku *% total*		% z uživatelů internetu *% of Internet users*	
	2005	2009	2005	2009
Česká republika	5.5	23.7	15.5	36.8

Obr. 6: Chování uživatelů – nákupy přes internet, zdroj: ČSÚ. *Nákupy přes internet*. 2010. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/nakupy_pres_internet/$File/7_nakupy_pres_internet.xls

3.3.2 Konkurence

Zde analyzuji konkurenční prostředí na trhu. Konkurenci v cílovém segmentu můžeme rozdělit na dvě hlavní skupiny - antivirové společnosti a nezávislé PC servisy.

3.3.2.1 Antivirové společnosti

Na trhu se pohybují 3 společnosti - AVG Technologies (AVG), Alwil Software (Avast) a ESET (ESET). Jedná se o velké nadnárodní společností s vysokým kapitálem.

Technická podpora od antivirových společností má velmi dobrou časovou i geografickou dostupnost. Technická podpora je zdarma, ovšem je k dispozici pouze pro uživatele placených produktů, kterých je menšina. Uživatelům bezplatných verzí antivirových produktů není technická podpora poskytována z kapacitních důvodů. Vzhledem k tomu, že většina uživatelů využívá bezplatné verze antivirových produktů, velká část trhu zůstává ze strany antivirových společností nepokryta.

3.3.2.2 Nezávislé PC servisy

Množinu zákazníků, kteří nemají nainstalován žádný antivirový produkt nebo používají verzi zdarma, se snaží pokrýt nezávislé PC servisy, které nabízejí opravu PC v kamenné prodejně nebo je možno objednat výjezd technika do bydliště zákazníka. Zde se fundamentálně mění podnikatelský model. Technická podpora není závislá na žádném placeném produktu, zpoplatněn je samotný servis.

Trh PC servisů není v současné době zmapován, proto jsem si udělal vlastní průzkum přes vyhledávače Seznam.cz a Google.cz. V Brně se aktuálně nachází 5 servisních společností, které se zaměřují na segment koncových uživatelů a vyvíjejí v této oblasti marketingovou aktivitu. Mezi tyto společnosti patří Computer Store s.r.o., Bartoš Viktor OSVČ (InDesign), Pavel Mucherl OSVČ (pcbrno.cz), Jiří Franz OSVČ (Fcomp), Ondřej Loner OSVČ (ict Loner). Ceny se pohybují od 290 Kč do 600 Kč za hodinu práce podle denní doby.

3.3.3 Nedostatky nabízených služeb

Zde uvádím nedostatky služeb, které jsou nabízeny na cílovém trhu.

3.3.3.1 Omezená geografická dostupnost

Lokální PC servisy jsou závislé na tom, že se zákazník nachází v jejich blízkosti. Z pohledu podnikatele není rentabilní vyslat technika z Prahy do Brna z důvodu vysokých výdajů na benzín a čas. Stejně tak zřizovat pobočky servisní společnosti v každém

větším městě je velmi nákladné a vzhledem k finančním možnostem lokálních PC servisů nerealizovatelné. Momentálně v České republice není žádná síť PC servisů, která by pokrývala více regionů.

3.3.3.2 Nízká efektivita

Další překážkou většího rozšíření servisních služeb pro koncové zákazníky je malá spolehlivost nabízených služeb. Toto platí hlavně u technické podpory ze strany antivirových společností. Technická podpora ze strany antivirových společností je prováděna přes telefon nebo e-mail. Tyto kanály jsou nevhodné pro řešení technických problémů, protože zákazník musí vykonat potřebné kroky sám dle instrukcí technika. Cílová zákaznická skupina nemá dostatečné technické znalosti pro pochopení instrukcí poskytnutých technikem přes telefon nebo e-mail.

3.3.3.3 Dlouhá reakční doba

U servisů PC se výrazně prodlužuje reakční doba, když je prováděn servisní zásah přímo na prodejně. Tato služba není prováděna na počkání, ale uživatel musí počítač v servisu nechat na dobu, která se pohybuje v řádu dní až týdnů. V případě technické podpory ze strany antivirových společností jsou zákazníci limitováni kapacitou call centra, kde se zpracovávají stovky nebo tisíce případů denně. Z mých zkušeností s prací na technické podpoře ve společnosti AVG Technologies se odezva na e-mailový požadavek zákazníka pohybuje rovněž v řádu dnů až týdnů.

3.4 Shrnutí analýzy

Segment zabezpečení počítačů a technické podpory koncových zákazníků má dlouhodobě rostoucí trend. S nástupem dial-up připojení a rozšířením cenově dostupné výpočetní techniky se začala rozšiřovat množina počítačových uživatelů bez technických znalostí. Tento segment uživatelů stále více využívá internet k činnostem jako je internetové bankovnictví a nákup zboží. Růst technické vzdělanosti v segmentu

je výrazně pomalejší než růst využití internetu. Uživatelé bez technického vzdělání kladou stále vyšší nároky na kvalitu technické podpory a zabezpečení jejich počítače.

V současné době jsou služby na trhu roztříštěné a nejednotné. Hlavní nevýhody poskytovaných služeb jsou nízká efektivita, omezená dostupnost a dlouhá reakční doba. Vzhledem k vysokým výdajům na provoz kamenných servisů není na trhu žádná nezávislá servisní společnost, která by pokrývala více jak jedno regionální město. Vzhledem k omezenému lokálnímu pokrytí trhu vzniká prostředí nedokonalé konkurence. Servisní služby nejsou standardizované z pohledu ceny a kvality. Důvodem nízké penetrace trhu jsou příliš velké fixní výdaje a nedostatek specializovaných pracovníků.

Telefonická a e-mailová podpora nadnárodních softwarových společností nestačí z kapacitních důvodů reagovat na potřeby trhu. Většina softwarových produktů v České republice technickou podporu nezahrnuje. V poskytování technické podpory a zabezpečení PC pro segment koncových zákazníků vzniká mezera na trhu, kterou je třeba zaplnit.

4. Teoretická východiska řešení

4.1 Typy počítačových infekcí

V této části práce se věnuji popisu existujících typů počítačových infekcí. Infekce jsou rozděleny do dvou základních kategorií. Do kategorie malware spadají viry, trojské koně, spyware a další typy infekcí. Samostatnou kategorií jsou rootkity. Rootkit je tak specifický a komplexní typ infekce, že je v odborné literatuře řazen odděleně od malware. Zde rootkity také popisuji v samostatné kategorii. Rootkity dnes představují nejmodernější typ infekce a jsou budoucností počítačové kriminality.

4.1.1 Malware

V této kapitole o malware jsem čerpal informace z [2].

Malware může být rozdělen na následující typy podle jeho funkčnosti. Antivirové aplikace dokážou detekovat všechny tyto typy malware. S popsanými typy malware souvisejí 2 charakteristické rysy:

a) *Sebe-replikace:* znamená, že se malware aktivně pokouší rozmnožovat vytvářením nových kopií sebe sama.

b) *Parazit*: malware vyžaduje jiný spustitelný kód, aby mohl fungovat.

4.1.1.1 Virus

Sebe-replikace: ano
Parazit: ano

Virus je malware, který se při spuštění snaží replikovat a vložit do jiného spustitelného kódu. Když uspěje, celý spustitelný kód je považován za infikovaný. Když je

infikovaný kód spuštěn, může obratem infikovat další kód. Tato metoda sebe-replikace do existujícího spustitelného kódu je charakteristická vlastnost definující virus. Virus se může šířit v rámci jednoho počítače, nebo na další počítače přes výměnná média jako je např. USB flash disk.

4.1.1.2 Červ

Sebe-replikace: ano
Parazit: ne

Červ sdílí několik charakteristických vlastností s virem. Nejdůležitější vlastnost červa je také sebe-replikace, ale u červa je sebe-replikace odlišná ve dvou aspektech. Za prvé, červy jsou samostatně fungující jednotky a nepotřebují k funkci jiný spustitelný kód. Za druhé, červy se šíří mezi počítači přes síť.

4.1.1.3 Zadní vrátka (backdoor)

Sebe-replikace: ne
Parazit: může být

Jako zadní vrátka je označován mechanismus, jehož cílem je obejít bezpečnostní kontrolu. Programátoři někdy vytváří zadní vrátka z legitimních důvodů, např. pro přeskočení zdlouhavého procesu autentizace během ladění síťového serveru. Zadní vrátka mohou být samostatná aplikace nebo součást legitimního kódu.

4.1.1.4 Trojský kůň

Sebe-replikace: ne
Parazit: ano

Trojský kůň je program, který se na pohled tváří, že vykonává nějakou legitimní činnost, ale ve skutečnosti na pozadí provádí škodlivou činnost bez povšimnutí

uživatele. Klasickým příkladem je program na krádež hesla, který uživateli zobrazí věrohodně působící přihlašovací okno, kde žádá login a heslo. Když uživatel zadá požadované údaje, program si je uloží a odešle tvůrci škodlivého kódu a uživateli vypíše hlášení, že bylo zadáno nesprávné heslo. Poté program spustí skutečné přihlašovací okno. Nic netušící uživatel si myslí, že se překlepnul při zadávání hesla a zadá znovu login a heslo. Poté je úspěšně přihlášen do systému, aniž by tušil, že byly odcizeny jeho přihlašovací údaje.

4.1.1.5 Spyware

Sebe-replikace: ne
Parazit: ne

Spyware je software, který sbírá informace z počítače a poté je odesílá někomu jinému. Informace, které spyware sbírá, mohou být různé. Většinou se jedná o data hodnotná pro útočníka:

a) Přihlašovací jména a hesla. Ty můžou být sbírána ze souborů uložených na počítači nebo pomocí keyloggeru, tj. programu, který zaznamenává veškeré stisknuté klávesy na počítači. Keylogger se liší od trojského koně tím, že jen pasivně zaznamenává stisky kláves, není přítomna žádná podvodná obrazovka pro klamání uživatele.

b) E-mailové adresy, které mají hodnotu pro spammery.

c) Čísla bankovních účtů a kreditních karet.

d) Licenční klíče softwaru, k usnadnění softwarového pirátství.

Viry a červy mohou sbírat podobné informace, ale nejsou považovány za spyware, protože spyware neobsahuje sebe-replikaci. Spyware se může dostat na počítač mnoha způsoby, např. jako součást softwarového balíčku, který si uživatel nainstaluje; nebo

využitím bezpečnostních děr v internetovém prohlížeči. Druhá z uvedených metod znamená, že pro nakažení spyware stačí, aby uživatel navštívil internetovou stránku. Spyware se do počítače v takovém případě stáhne, aniž by o tom uživatel věděl a aniž by musel vykonat na stránce jakoukoliv akci, stačí pouhá návštěva stránky.

4.1.1.6 Adware

Sebe-replikace: ne
Parazit: ne

Adware je podobný spyware. Také sbírá informace o uživateli a jeho chování. Adware je více marketingově zaměřený a může uživateli na PC zobrazovat vyskakující pop-up okna nebo přesměrovávat internetový prohlížeč uživatele na různé komerční stránky za účelem navedení uživatele k nákupu na těchto stránkách. Některý adware se snaží cílit reklamy zobrazované uživateli podle toho, co uživatel na počítači dělá. Např. pokud uživatel vyhledává na Seznamu výraz "Škoda", adware může začít zobrazovat reklamní okna "levné náhradní díly pro automobily Škoda".

Adware může také sbírat a odesílat data o uživatelích, které jsou poté vyžity pro marketingové účely. Tak jako spyware, adware nepodporuje sebe-replikaci.

4.1.1.7 Logická bomba

Sebe-replikace: ne
Parazit: může být

Logická bomba je kód, který se skládá ze dvou částí:

a) Nálož: akce, která se má vykonat. Nálož může být cokoliv, ale nejčastěji se jedná o akci se škodlivým efektem.

b) Spoušť: matematická podmínka, která je kontrolována. Podle ní se určuje, kdy je nálož "odpálena". Spouštěcí podmínka může být prakticky cokoliv, často se používají hodnoty jako datum, přihlášení uživatele do systému nebo verze operačního systému.

Logická bomba může být vložena do existujícího kódu nebo může jít o samostatný kód.

4.1.2 Rootkity

V této kapitole o rootkitech jsem čerpal informace z [1].

Rootkit není software v pravém slova smyslu. Rootkit můžeme definovat jako "nedetekovaný soubor programů a zdrojového kódu, který umožňuje konstantní přítomnost na počítači nebo v informačním systému". Na rozdíl od malware, rootkit je v systému stále aktivní i po restartu operačního systému, zatímco malware funguje jen za běhu systému a po restartu už není aktivní. Toto je klíčový rozdíl mezi malware a rootkity. Rootkity jsou záměrně psány tak, aby nebyly detekovány tradičními metodami, které využívají antivirové společnosti. Většina dřívějších infekcí se nezaměřovala na skrytí jejich existence v systému, rootkit je první typ infekce, u níž je vyhnutí se detekci hlavním cílem.

Obecně existují dva typy rootkitů: user-mode rootkity a kernel-mode rootkity. User-mode rootkity běží v prostředí a a bezpečnostním kontextu uživatele systému. Uživatel se anglicky řekne "user", z toho označení user-mode rootkit. Když jste přihlášeni na počítači např. jako uživatel Franta a nemáte práva administrátora, rootkit vyfiltruje a poskytne přístup ke všem aplikacím běžícím pod účtem Franta. Rootkit Vám tedy neposkytne přístup k aplikacím a službám, ke kterým nemá přístup uživatel Franta. Ovšem v dnešní době má většina uživatelů na počítačích administrátorská práva, takže pokud user-mode rootkit infiltruje počítač s právy právě přihlášeného uživatele, většinou tak získá administrátorský přístup ke všem službám a aplikacím.

Kernel-mode rootkity operuje na úrovni jádra operačního systému stejně jako ovladače hardwaru. Kernel je anglické označení pro jádro, odtud označení kernel-mode rootkit. Během psaní bakalářské práce budu střídavě používat označení kernel a jádro, jedná se o totéž. Napsat (vyvinout) rootkit pro operaci na úrovni kernelu operačního systému je mnohem obtížnější než napsat user-mode rootkit a vyžaduje mnohem vyšší schopnosti implementace ze strany útočníka. Je také důležité zmínit, že kernel-mode rootkity nefungují na všech verzích Windows, protože Microsoft většinou mění nebo upravuje různé části kernelu s každým updatem a novou verzí operačního systému. Jelikož kernel-mode rootkit funguje v kernelu stejným způsobem jako ovladač, má také tendenci zvyšovat nestabilitu operačního systému. Toto je obvykle jak většina lidí zjistí, že mají na počítači rootkit. Většinou se kernel-mode rootkit projeví zpomalením počítače, snížením výkonu, nebo se začne objevovat modrá obrazovka smrti nebo další chyby, které způsobují samovolné restartování systému.

4.1.2.1 User-mode rootkit

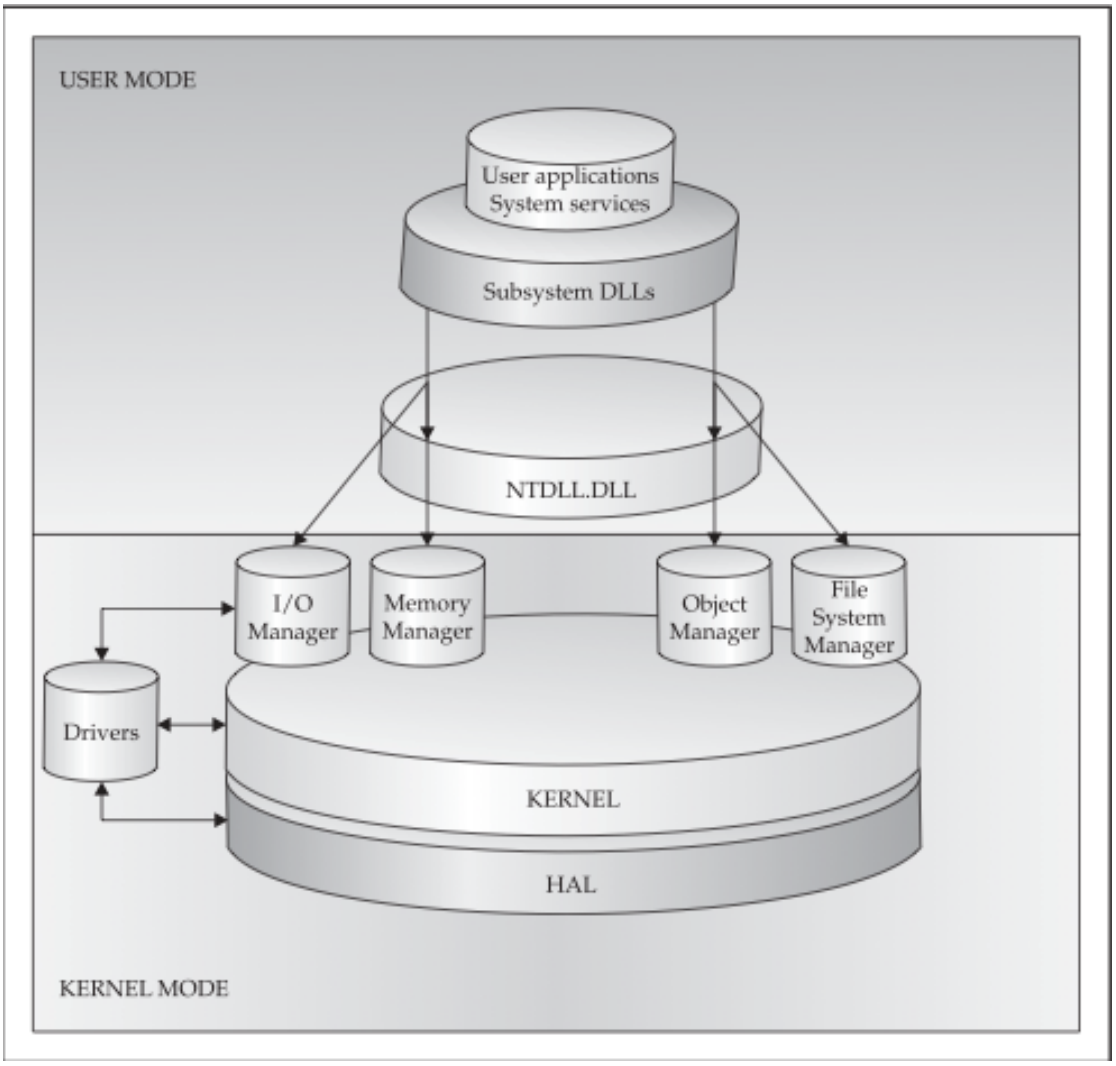
Na základě definice uvedené v předchozí sekci můžeme user-mode rootkit označit jako " nedetekovaný soubor programů a zdrojového kódu, který běží pod uživatelskými právy, a umožňuje konstantní přítomnost na počítači nebo v informačním systému". Uživatelskými právy jsou v tomto případě myšlena práva jakéhokoliv uživatele systému, včetně administrátora. User-mode rootkit tedy přístup ke všem aplikacím, ke kterým má přístup aktivní uživatel. Rootkit může přistupovat jen tam, kam může přistupovat uživatel, pokud nemá uživatel povolení pro zápis do složky Program Files nebo Windows, nemá toto povolení ani rootkit. Ovšem protože většina běžných uživatelů počítačů je do systému přihlášena s administrátorskými právy, rootkit infiltrující takového uživatele tak získává přístup s neomezenými právy v rámci uživatelského prostředí v operačním systému. Uživatelským prostředím je v tomto případě myšleno prostředí uživatele "administrátor". Důležité je ale zmínit že user-mode rootkit nemá přístup do kernelu operačního systému a stále se na něj vztahují veškerá omezení a politiky, například omezená přístupová práva k systémovým souborům.

Z důvodu popularity operačního systému, velkého množství volně přístupného zdrojového kódu, a rozsáhlé dokumentace oficiálních hooking mechanismů je vývoj user-mode rootkitů velmi jednoduchý. I přes jednoduchost vytvoření vlastního rootkitu se většina útočník rozhodla, že stáhnutí nějakého zdrojového kódu a jeho kompilace je příliš časově náročná, a radši si koupí hotový rootkit. Rozsáhle používaný a efektivní user-mode rootkit Hacker Defender je na internetu možné koupit za přibližně 500 amerických dolarů. Zdrojový kód rootkitu Hacker Defender a jiných user-mode rootkitů je volně ke stažení pro případ, že byste si ho chtěli stáhnout a upravit pro tvorbu vlastního rootkitu. Open-source rootkity se stali velmi běžné a nyní je tak snaží pro nezkušené útočníky vytvořit si vlastní rootkit a vstoupit do světa počítačové kriminality.

Zkrácení času pro tvorbu rootkitu a jeho infiltrace do Windows napomohlo šíření malware, který využívá user-mode rootkit k ukrytí v systému. Malware se může díky rootkitu ukrýt před správcem úloh systému Windows, před registry i před souborovým systémem (nenajdeme malware přes správce úloh, registry ani průzkumník). Protože se user-mode rootkity rychle rozšířili, antivirové společnosti začali přicházet s novými technikami jak je detekovat. Dnes nejsou user-mode rootkity příliš efektivní a jsou relativně snadno detekovatelné většinou antivirových programů. Ovšem mnoho kusů malware user-mode rootkity stále využívá, takže je stále důležité sledovat a analyzovat jejich vývoj.

4.1.2.2 Kernel-mode rootkit

Kernel-mode rootkity existují pro velké množství operačních systémů od Linuxu po Mac OS X. V této kapitole popisuji fungování kernel-mode rootkitu v kontextu operačního systému MS Windows s architekturou x86, který je nejrozšířenější. Pro pochopení funkce kernel-mode rootkitu je třeba vědět, jak vypadá architektura operačního systému MS Windows a jak funguje jádro systému. Popis celé architektury a jádra MS Windows by vydal na samostatnou bakalářskou práci, takže v této kapitole je jen velmi stručně nastíněno, jak kernel-mode rootkity fungují. Architektura systému MS Windows je přehledně znázorněna na obrázku č. 7.



Obr. 7: Architektura systému MS Windows, zdroj: DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. 2010. s. 125

Kernel-mode rootkit je pravděpodobně nejstarší a nejvíce se vyskytující typ rootkitu. Dnes představuje největší hrozbu z hlediska počítačové bezpečnosti. Např. červ StormWorm, který infikoval stovky tisíc počítačů v roce 2007, v sobě obsahoval kernel-mode rootkit komponentu. Právě tato kernel-mode rootkit komponenta umožnila červu napáchat více škod než jiné infekce a hlavně umožnila infikovat počítač na velmi nízké úrovni - na úrovni operačního systému.

Kernel-mode rootkity jsou jednoduše škodlivé instrukce, které běží na nejvyšším privilegovaném stupni CPU v jádře operačního systému. Jádro má nejvyšší prioritu pro zasílání instrukcí CPU, tím pádem mají nejvyšší prioritu i instrukce zaslané kernel-mode rootkitem. Tak jako user-mode rootkit, musí mít kernel-mode rootkit spouštěcí

instrukci. Ta může být v podobě nahratelného kernel modulu (.dll) nebo ovladače zařízení (.sys), který je nahrán přímo spouštěcím programem nebo nějakým způsobem zavolán operačním systémem. Jakmile je ovladač nahrán, rootkit je zaveden v kernelu a může začít modifikovat funkcionalitu operačního systému.

Většina kernel-mode rootkitů má určité vlastnosti, kvůli kterým je složité rootkit objevit a odstranit. Tyto vlastnosti jsou následující:

a) Utajenost (stealth): Získat přístup do kernelu je velmi složité. Tvůrce rootkitu, který je dostatečné zkušený, aby dokázal přístup do jádra získat, je i dostatečně zkušený na to, aby zajistil, že rootkit bude fungovat bez povšimnutí uživatele.

b) Vytrvalost (persistence): Jeden z hlavních cílů rootkitu je, aby byl neustále přítomen v systému. Pokud rootkit není konstantně aktivní, nemá pro jeho tvůrce cenu trávit tolik času jeho psaním. Takže kernel-mode rootkity jsou většinou velmi dobře promyšlené a zahrnují funkce, které zajistí, že rootkit dokáže přežít restart počítače. Rootkit je také odolný vůči detekci a odstranění, tím způsobem, že jakmile zjistí, že je snaha o jeho odstranění, automaticky se replikuje za pomocí nejrůznějších technik.

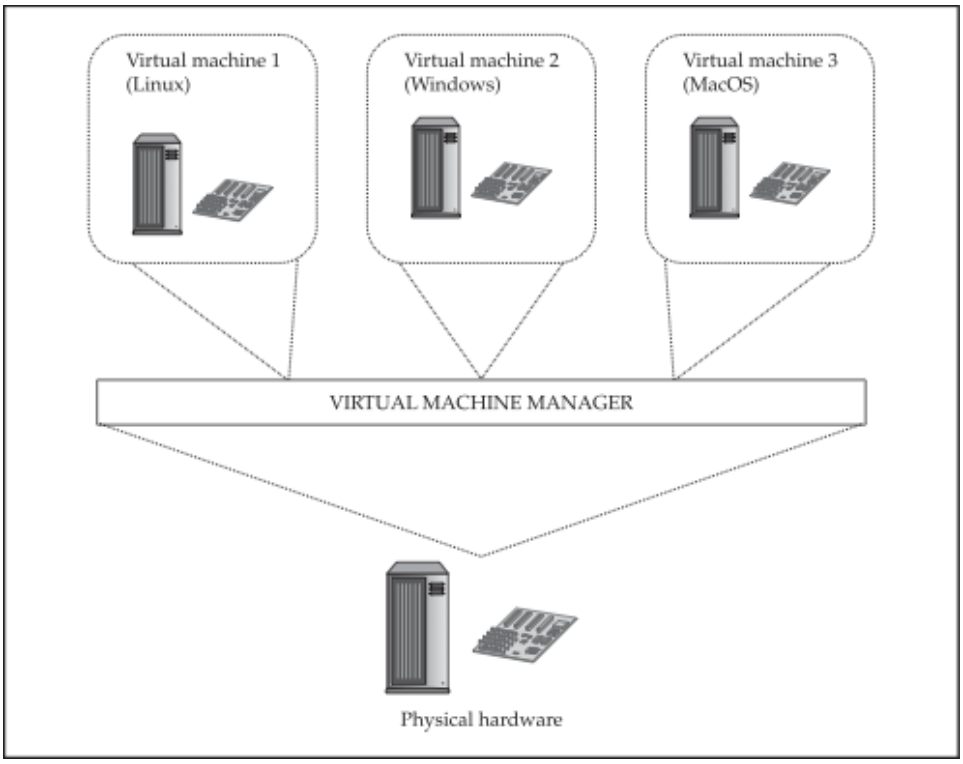
c) závažnost (severity): Kernel-mode rootkity využívají pokročilých technik k narušení integrity operačního systému. Toto má vliv nejen na stabilitu systému (časté pády nebo snížení výkonu počítače), ale také odstranění infekce a obnovení systému do původního stavu je mnohem složitější než u jiných typů infekce.

4.1.2.3 Virtuální rootkit

Virtualizační technologie jsou dnes stále více populární v síťových infrastrukturách. S nárůstem užití těchto technologií se zvyšuje i procento virtuálních rootkitů, které v

současné době představují nejmodernější formu rootkit technologie. Technické mechanismy, na kterých funguje virtualizace, zároveň umožňují napadení systému způsoby, které dříve nebyly možné. Hardwarová a softwarová podpora virtualizace se za posledních pár let několikanásobně zvýšila, což nahrává útočníkům, kterým se tak otevřela úplně nová cesta pro infikování systému.

Virtualizace dovoluje jednomu fyzickému počítači sdílet zdroje mezi několika operačními systémy, které běží souběžně. Virtualizace se využívá hlavně v prostředí serverů, kde umožňuje paralelizaci a sdílení zdrojů, což vede ke zvýšení produktivity. Princip virtualizace je znázorněn na obrázku č. 8.



Obr. 8: Virtualizace systémových zdrojů, zdroj: DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. 2010. s. 175

Virtuální rootkit je napsán a navržen specificky pro virtualizační prostředí. Jeho cíl je stejný jako u ostatních typů rootkitů popsaných výše (utajenost, vytrvalost, závažnost). Komponenty jsou také stejné, ale technika rootkitu je naprosto odlišná. Hlavní rozdíl spočívá v tom, že virtuální rootkit se již nezaměřuje na modifikaci samotného operačního systému, ale na jeho transparentní korupci uvnitř virtuálního prostředí. Ve

zkratce, virtuální rootkit obsahuje funkcionalitu detekce virtuálního prostředí a může z něj volitelně uniknout. Stejně tak se může nabourat do mateřského operačního systému a nainstalovat zde škodlivý hypervisor. Bojiště virtuálních rootkitů se tak přesouvá z úrovně operačního systému na úroveň pod operačním systémem. Zatímco tradiční rootkit (user-mode a kernel-mode) se musí snažit nacházet nové způsoby jak bez povšimnutí modifikovat operační systém, virtuální rootkit se operačního systému nemusí ani dotknout. Virtuální rootkit jen využije virtualizační podpory, kterou nabízí hardware a software, a infiltruje se pod operační systém.

Virtuální infekce můžeme rozdělit na 3 typy:

a) Virtualization-aware malware (VAM): tohle je běžný malware, který má navíc schopnost detekce virtuálního prostředí a může ho napadnout.

b) Virtual machine-based (VMB) rootkit: tradiční typ rootkitu, který má schopnost obalit virtuální operační systém bez jeho vědomí. Toho je dosaženo modifikací existujícího virtualizačního softwaru.

c) Hypervisor virtual machine (HVM) rootkit: tento rootkit využívá hardwarové virtualizační podpory pro kompletní přepsání hypervisoru vlastní modifikovanou verzí. Poté může rootkit za běhu modifikovat virtuální i mateřský operační systém.

4.1.2.4 Budoucnost rootkitů

Rootkity se začínají vyvíjet jako viry před 10 - 20 lety, kdy se postupně z virů začal tvořit spyware, adware atd. Vytvořit vlastní rootkit je momentálně technicky náročná činnost, takže mnoho méně zdatných útočníků rootkity nevyužívá z důvodu jejich složitosti. To se ale začíná měnit. Tvůrci rootkitů začínají balit jejich rootkity do modulů a začínají vzdělávat útočníky, aby uměli jejich rootkity používat (jak jsme si vysvětlili dříve, tvůrce rootkitu a útočník většinou není jedna a ta samá osoba).

Snadnější dostupnost zdrojového kódu rootkitů na stránkách jako je rootkit.com je další faktor, který usnadňuje přístup k rootkitům méně zkušeným útočníkům.
Z pohledu vývoje je nejklíčovější schopnost rootkitů utajenost. Rootkity budou postupně vylepšovat své schopnosti utajenosti, aby se vyhnuli detekci ze strany nejnovějších anti-rootkit nástrojů. Bez detekce bude moci rootkit netušeně škodit v operačním systému. Na rozdíl od období kolem roku 2000, kdy se výrobci operačních systémů příliš nesoustředili na bezpečnost, se nyní mění zaměření a je věnováno mnohem větší úsilí a finanční prostředky na zabezpečení jednotlivých komponent operačních systémů. S vydáním nových operačních systémů jako je Windows 7 nebo Windows Server 2008, rootkity budou mít nyní těžkou práci s infiltrací jádra nebo uživatelského rozhraní systému a začnou se pravděpodobně zaměřovat na aplikace výrobců třetích stran.

Detekce rootkitu je ale jen jedna část úspěchu. Postupem času se totiž bude zlepšovat také vytrvalost rootkitu. Rootkity budou aplikovat nové metody, které zajistí, že nebude možné rootkit smazat, a pokud ano, tak to může způsobit ztrátu dat nebo nestabilitu systému. Antivirové společnosti budou muset začít aplikovat "odzbrojující" proces, více než "čistící" proces, který je používán nyní. Čistící proces spočívá v odstranění všech infikovaných souborů. Pokud ale rootkit infikuje systémový soubor, není možné na něj aplikovat klasický čistící proces, protože systémový soubor nemůžeme jen tak odstranit. Čistící proces je časově náročný a náchylný k chybám. Může snadno dojít k tomu, že jeden ze sady souborů rootkitu nebude detekován, a rootkit se poté z toho souboru může zpátky rozšířit do systému. Odzbrojení rootkitu znamená, že zablokujeme hlavní funkcionalitu rootkitu. Tím pádem rootkit nemůže fungovat a spouštět další škodlivé programy a stává se tak neškodným.

4.2 Metody prevence a zabezpečení

Popisované metody zabezpečení a prevence jsou integrovány v komerčních antivirových aplikacích, které dnes má většina uživatelů a firem nainstalovaných na svých počítačích. Metody jsem rozdělil podle typů infekcí do dvou skupin.

4.2.1 Detekce malware

V této kapitole o detekčních technikách malware jsem čerpal informace z [2].

Detekce malware se z technologického hlediska dále dělí na statické a dynamické metody. Statické metody pro detekci malware jsou základním kamenem všech dnes existujících komerčních antivirových aplikací, ať už se jedná o verzi zdarma nebo placenou verzi. V posledních letech začínají společnosti do svých aplikací integrovat i komponenty pro dynamickou detekci, které zatím nejsou tak efektivní a představují spíše něco funkci navíc. Dynamické metody detekce představují budoucnost vývoje detekčních technik malware a většina společností pracuje na zlepšování dynamické detekce v jejich produktech.

4.2.1.1 Statická detekce

Statická detekce se snaží najít infekci, aniž by se spouštěl skenovaný kód. Existují 3 hlavní techniky statické detekce: skenery, statická heuristika a kontrola integrity.

Skenery

Skener je v oblasti detekce malware slovo používané velmi obecně, analogicky ke slovu virus pro pojmenování infekce. Ale stejně jako označení virus ve smyslu infekce, je skener ve skutečnosti jen jeden specifický typ detekce malware, nikoliv obecné označení pro jakoukoliv aplikaci.

Skenery se rozdělují do dvou skupin, podle způsobu spuštění skeneru:

a) On-demand skener: je vždy spuštěn uživatelem počítače. Často se tento typ skeneru dá nastavit jako plánovaný, aby se spouštěl periodicky například každý týden. Také se dá nastavit jaké složky a typy souborů se mají skenovat.

b) On-access skener: je neustále aktivní systému a testuje každý spuštěný soubor. S tímto skenerem je spojena větší hardwarová zátěž a tím pádem

snížení výkonu počítače. Většinou bývá k dispozici i nastavení skeneru, které umožňuje zvolit jaká akce se má vykonat při nalezení infekce, zda se mají soubory testovat při uzavírání apod.

Každý skener má vlastní databázi, kde je každá infekce reprezentována sekvencí bajtů, které unikátně charakterizují virus. Tato sekvence je většinou tvořena jedním nebo více kusy zdrojového kódu infekce nebo podpisem (skenovacím řetězcem). Skener pak prochází celou zvolenou oblast (například složku nebo celý pevný disk) a všechny skenované soubory porovnává vůči své databázi. Když nalezne shodu, označí soubor jako infikovaný. Poté buď infekci oznámí uživateli, nebo ji automaticky odstraní nebo přesune do truhly, podle nastavení skeneru.

Tento typ detekce dokáže najít pouze již známé viry, které byly před skenováním přidány do databáze.

Statická heuristika

Anti-virový software může použít statickou heuristiku pro zvýšení úspěšnosti detekce. Statická heuristika dokáže odhalit známé nebo neznámé infekce tím, že hledá kusy kódu, které jsou "virus-like", namísto hledání konkrétních sekvencí kódu. Tato metoda je statická, což znamená, že skenovaný kód není spuštěn.

Statická heuristika probíhá ve dvou krocích:

a) Sběr dat: data mohou být získána jakýmkoliv statickým skenerem. Skener většinou hledá krátké podezřelé řetězce, které se nazývají boostery. Přítomnost boosteru obvykle zvyšuje šanci, že je analyzovaný kód škodlivý. Stejně důležité jako hledání podezřelých řetězců je hledání aspektů, které naopak infekci vylučují. Například škodlivé programy většinou nezobrazují dialogová okna s dotazem uživateli. Takovýmto řetězcům se říká stoppery.

b) Analýza dat: bere se v úvahu počet nalezených boosterů a stopperů s souboru. Dle přítomnosti těchto řetězců je poté každému souboru přiřazeno určité hodnocení. Forma detekce je pak jen jednoduše nastavení určité bodové hranice, nad kterou už je soubor označen jako škodlivý.

Kontrola integrity

Infekce obvykle fungují tím způsobem, že modifikují jiné korektní soubory. Kontrola integrity hledá neautorizované změny souborů a na základě těchto změn poté detekuje infekci. Kontrola integrity se musí začít provádět na čistě nainstalovaném systému, který na 100% není infikován. Kontrolor integrity si při svém prvním spuštění uloží kontrolní hodnoty (check-sum) všech souborů, které sleduje. Při další kontrole je kontrolní hodnota znovu vypočítána pro každý soubor a porovnána s původní hodnotou. Pokud se hodnoty liší, proběhla změna souboru a tím pádem je zde podezření na infekci.

4.2.1.2 Dynamická detekce

Techniky využívající dynamickou detekci vždy spustí kontrolovaný kód a monitorují jeho chování. Na základě analýzy chování poté vyhodnotí, zda je soubor infikován.

Kontrola chování

Kontrola chování je metoda, kdy antivirový software monitoruje chování běžícího programu v reálném čase. Pokud odhalí podezřelou aktivitu, kontrolor chování zabrání provedení podezřelých operací, ukončí program nebo se zeptá uživatele, jakou akci má provést. Kontrola chování (behavioral monitor) se někdy také nazývá blokace chování (behavioral blocker).

Emulace

Kontrola chování monitoruje kód, který reálně běží na počítači. Naproti tomu,

antivirové techniky užívající emulaci nespouští kód přímo na počítači, ale v emulovaném (virtuálním) prostředí. Cíl je v emulovaném prostředí zjistit, zda spuštěný program vykazuje známky infekce. Protože veškerý kód běží ve virtuálním prostředí a ne přímo na počítači, není napáchána žádná škoda v případě, že je program infikovaný.

Emulace lze provádět dvěma způsoby, ačkoliv rozdíl mezi nimi není příliš viditelný:

a) Dynamická heuristika: je stejná jako statická heuristika. Jediný rozdíl je způsob shromáždění dat pro analýzu. Dynamická heuristika získává data z emulátoru, ve kterém je spouštěn testovaný kód. Samotná analýza pak probíhá stejně jako u statické heuristiky.

b) Generické dešifrování:u polymorfních infekcí může být velmi těžké najít známky podezřelého chování. Generické dešifrování obchází tento problém tak, že se spoléhá na dešifrovací modul samotné infekce, aby dešifrovala sebe sama a antivirový software tak mohl odhalit infikovaný kód nebo škodlivé chování.

4.2.2 Detekce rootkitů

V této kapitole o detekčních technikách rootkitů jsem čerpal informace z [1].

4.2.2.1 MS Windows anti-rootkit techniky

Microsoft za posledních 10 let investoval velké množství času a finančních prostředků na zlepšení zabezpečení všech verzí od Windows XP Service Pack 3 výše. V roce 2005 Microsoft představil novou sadu technologií, která podporuje zlepšování systémové bezpečnosti. Mezi tyto technologie patří:

a) Secure development lifecycle (SDL): zahrnutí nových bezpečnostních procedur do vývojářského procesu.

b) Windows service hardening: Microsoft Windows nyní spouští více služeb jádra s omezenými privilegii, takže pokud malware získá kontrolu nad danou službou, operační systém zabrání eskalaci privilegií služby.

c) No-execute (NX) a address space layout randomization (ASLR): tyto dvě techniky byly přidány hlavně pro prevenci přetečení zásobníku, což je škodlivá technika, kterou často používají rootkity.

d) Kernel patch protection (KPP): předchází tomu, aby jakýkoliv program modifikoval kernel nebo data struktury kernelu jako SSDT nebo IDT.

e) Required driver signing: na 64-bitových systémech musí být všechny kernel-mode ovladače digitálně podepsány ověřenými entitami. Nepodepsané ovladače nejsou do systému nahrány.

f) BitLocker drive encryption: řešení zajišťující zašifrování celého pevného disku na počítači.

g) Authenticode: umožňuje vývojářům třetích stran podepsat jejich aplikace. Kernel následně kontroluje hash kód aplikace, zda je stejný jako kód zaslaný výrobcem aplikace.

h) Software restriction policy: tato technologie je vhodná pro firemní softwarovou kontrolu. Pokud administrátor nepovolil instalaci určitého softwaru do systému, tak se ho žádnému uživateli ve firemní síti nepodaří nainstalovat.

4.2.2.2 Software-based detekce

Mnoho anti-rootkit aplikací je dnes dostupných na internetu ke stažení. Většina velkých antivirových společností začíná integrovat anti-rootkit komponenty do svých aplikací. Nástroje pro detekci rootkitů také existují v samostatné podobě. Jedná se o specializované aplikace, které nejsou vyvíjeny pro komerční účely. Nástroje pro detekci

rootkitů jsou často vyvíjeny buď nezávislými týmy IT specialistů či uzavřenými komunitami. Některé komerční antivirové společnosti nabízejí samostatné nástroje pro detekci rootkitů pro stažení zdarma. Momentálně je detekce rootkitů velmi komplexní proces a úspěšnost detekce rootkitů je velmi nízká. Proto žádná společnost neprodává samostatnou aplikaci pro detekci rootkitů, ale nabízí ji ke stažení zdarma.

Detekce rootkitů je velmi komplexní činnost, neexistuje žádný univerzální způsob detekce. Většina anti-rootkit nástrojů odhaluje rootkity tím způsobem, že detekuje tzv. hooks na různých komponentách v kernelu operačního systému. Většinou se jedná o komponenty tabulky SSDT nebo IDT, přes které jsou posílány různé instrukce z uživatelského prostředí do jádra systému a zpátky. Rootkit funguje tím způsobem, že modifikuje nebo přidává instrukce jdoucí přes tyto tabulky. Této modifikaci se říká hooking. Například anti-rootkit nástroj VICE detekuje hooks rozložením funkčních ukazatelů jdoucí přes kernel tabulku SSDT a kontroluje, zda ukazatele odkazují na správnou aplikaci. Každý nástroj pro detekci rootkitů využívá jinou metodu detekce. Pro odhalení rootkitu je tedy nejúčinnější zkombinovat více nástrojů.

4.2.2.3 Hardware-based detekce

Software-based detekce funguje tak, ze spustíme jeden program a pomocí něj se pokoušíme najít jiný škodlivý program. Vzhledem k tomu, že oba programy musejí bojovat o stejné prostředky a zařízení, je poměrně složité zajistit úspěšnou software-based detekci. Pokud selže detekce rootkitu pomocí softwaru, proč nezkusit hardwarovou detekci? Společnost Komoku právě takovou detekci implementovala. Společnosti Komoku, založena roku 2004, byla financována ministerstvem obrany a námořnictvem Spojených Států za účelem vytvoření hardware-based řešení detekce rootkitů. Společnost vyvinula hardwarové řešení zvané CoPilot. Jedná se o PCI kartu schopnou monitorovat operační paměť a souborový systém počítače na hardwarové úrovni. CoPilot skenuje paměť operačního systému téměř v reálném čase a namísto konkrétního kódu hledá v paměti nesrovnalosti. Vláda USA vydala prohlášení, že nasazení PCI karty CoPilot bylo úspěšné, ale protože je vývoj financován vládou, karta

CoPilot není dostupná pro veřejnost. Společnost Komoku byla v roce 2008 koupena společností Microsoft formou akvizice.

4.2.2.4 Detekce virtuálních rootkitů

Přítomnost virtuálního rootkitu na PC se zjišťuje tím, zda je v systému přítomna virtualizace. Pokud je počítač schopný provádět virtualizace, virtualizace není aktuálně spuštěna, ale je detekována přítomnost VMM (virtualizační manažer), pak je v systému virtuální rootkit.

5. Návrh řešení

5.1 Model poskytování služeb online

Obr. 9: Firemní logo, zdroj: vlastní

Do budoucna budou uživatelé počítačů a dalších technických zařízení vyžadovat rychlou a efektivní technickou podporu dostupnou na globální úrovni, nikoliv jen v Brně, ale také v dalších regionálních i menších městech. Je tedy třeba vytvořit obchodní model, který bude mít širší geografické pokrytí a zároveň bude adresovat nedostatky služeb uvedené v předchozí kapitole. Na základě analýzy trhu a zkušeností po roce podnikání v oblasti zabezpečení počítačů jsem sestavil nový koncept zabezpečení PC pomocí vzdáleného připojení, které odpovídá novým požadavkům cílových zákazníků.

Ve firemním sektoru již započal přechod na online poskytování služeb v oblasti technické podpory a zabezpečení. Většina nadnárodních společností technologie vzdáleného připojení pro servis výpočetní techniky svých zaměstnanců uvnitř společnosti či rovnou outsourcují správu a zabezpečení jejich systémů na externí společnosti. Mezi společnosti využívající tyto technologie patří např. AMD, HSBC, Symantec, Vodafone nebo AVG.

5.2 Výhody online modelu

V kapitole analýzy trhu jsme identifikovali několik slabých míst, které brání masovému rozšíření poskytovaných služeb. Omezená geografická dostupnost, dlouhá reakční doba

a nízká efektivita vyřešení problému. Všechny tyto nedostatky se dají eliminovat či zmírnit přechodem na online model poskytování služeb.

5.2.1 Pokrytí většího trhu

Použití modelu vzdáleného připojení výrazně zvýší naší geografickou dostupnost. Nyní jsme schopni pokrýt všechny zákazníky v České republice i v zahraničí z jednoho servisního místa. To výrazně zvětšuje základnu našich potencionálních zákazníků a tím i potencionální zisk z podnikatelské činnosti.

Každý koncový uživatel PC bez technických znalostí, který má připojení k internetu, se nyní stává potencionálním zákazníkem. „K datu září 2009 bylo k internetu v ČR připojeno 6,8 milionu uživatelů“[2]. Přibližně polovina připojení z tohoto počtu jsou středně velké a velké firmy, na které se nezaměřujeme. Z průzkumu znalostí uživatelů vyplývá, že 38% uživatelů má dostatečné technické znalosti, aby si počítač zabezpečili sami. V cílovém segmentu se tedy nachází přibližně 2,1 milionu potencionálních zákazníků. Kromě velikosti trhu je velmi dobrý i potenciál růstu, jak je vyobrazeno v průzkumech analýzy trhu. Poskytováním služeb online jsou pro mě dosažitelní zákazníci po celé ČR a také je snadné expandovat do zahraničí.

5.2.2 Zvýšení efektivity

Zavedením online připojení vzroste efektivita služeb. Nyní se mohu připojit paralelně k více zákazníkům. V plánu je vytvořit jednotlivé support úrovně. Nevyřešené případy je možné efektivně eskalovat v rámci organizace bez časových prodlev na zkušenější techniky. Zatímco u fyzického výjezdu účast dalšího technika není možná, nebo je velmi zdlouhavá, u vzdálené podpory můžeme plynule eskalovat problémy zákazníků a tím docílit vyšší efektivity vyřešení problémů. To povede k větší spokojenosti zákazníků a jejich loajalitě.

[2] JANOUCH V. *Internetový marketing Prosaďte se na webu a sociálních sítích*. 2010. s. 16

5.2.3 Snížení reakční doby

Servisními zásahy online se výrazně sníží reakční doba pro vyřešení problému zákazníka. Při fyzickém výjezdu trval průměrně 30 minut příjezd technika na místo a navíc jsme byli omezeni na Brno a okolí. Při vzdáleném připojení je reakční doba 5 - 10 minut bez omezení na oblast města Brna. Tento fakt výrazně zvyšuje atraktivitu služby z pohledu zákazníka.

5.2.4 Snížení výdajů

Poskytováním služeb online dosáhneme výrazného snížení výdajů. Při fyzických výjezdech k zákazníkovi jsme potřebovali automobil a vznikali nám výdaje na benzín. Vysoké výdaje na automobil a benzín bránili expanzi našeho podnikání. Přechodem na online služby naprosto odpadá nutnost těchto výdajů. Všichni pracovníci budou pracovat z domu, případně v dlouhodobějším horizontu budou umístěni na jednom pracovišti.

5.2.5 Efektivnější řízení

Společně se snížením výdajů vzniká další výrazná výhoda poskytování služeb online, a tou je centralizace. Online servis je možné provádět z jednoho místa, kde se budou nacházet všichni pracovníci. V dlouhodobém horizontu online model výrazně usnadňuje komunikaci, výměnu firemních informací a řízení pracovníků. Snižují se výdaje na telefon a dopravu, které bychom museli vynaložit na řízení pracovníků v jednotlivých městech.

5.3 Realizace přechodu na online model

Namísto fyzického výjezdu k zákazníkovi mu vysvětlíme jak spustit aplikaci pro vzdálené připojení a připojíme se přes vzdálenou plochu. Tímto způsobem můžeme

nabízet služby v oblasti řešení softwarových problémů, které mají majoritní podíl na trhu, jak jsme uvedli v analýze trhu.

5.3.1 Zakoupení aplikace pro vzdálené připojení

Pro poskytování servisních služeb na dálku je klíčové používat spolehlivou a uživatelsky jednoduchou aplikaci, přes kterou bude spojení realizováno. Po analýze dostupných aplikací pro vzdálené připojení jsem zvolil aplikaci LogMeIn Rescue od společnosti LogMeIn, Inc. Tato společnost prodává komerční aplikaci, která realizuje vzdálené připojení mezi technikem a koncovým zákazníkem. Aplikace byla vyvinuta pro účel vzdálené podpory, takže je velmi jednoduchá pro použití ze strany zákazníka a obsahuje potřebnou funkcionalitu pro mne jako servisního technika.

Mezi další aplikace, které umožňují vzdálené připojení patří GoToAssist, Teamviewer a Crossloop. Aplikace LogMeIn Rescue je z těchto čtyř produktů nejdražší, nabízí také ale nejlepší funkcionalitu, nejstabilnější spojení a funguje kompletně „in-the-cloud“. Z těchto důvodů jsem ji zvolil i přes vysokou cenu. Výdaje na aplikaci LogMeIn Rescue činní 1188 USD (20 527 Kč podle kurzu ke dni 22.5. 2011) ročně na jednu licenci.

Funkcionalita aplikace LogMeIn Rescue zahrnuje:

- podporu vzdáleného připojení na stanice s Windows, Mac OS X a na chytré telefonní přístroje bez nutnosti před-instalace software na straně zákazníka

- plně konfigurovatelný user interface, tak abychom mohli software personifikovat pro potřeby našeho podnikání

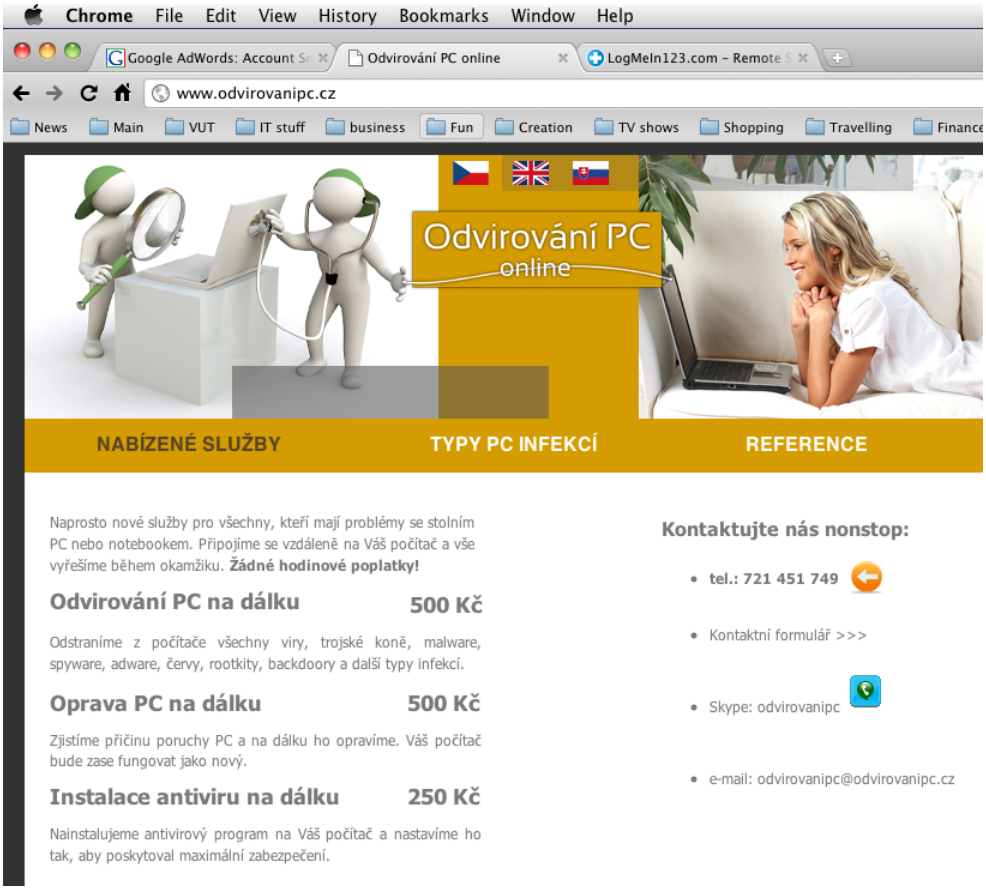
- možnost navázat až 10 paralelních spojení. Je tedy možné se v jednom okamžiku připojit až k 10 zákazníkům a jednoduše se mezi nimi přepínat v rozhraní aplikace

- „drag and drop“ kopírování souborů a složek na počítač / z počítače zákazníka přes integrovaný souborový manažer

- zabezpečení datové komunikace pomocí 256 bitové šifry typu AES

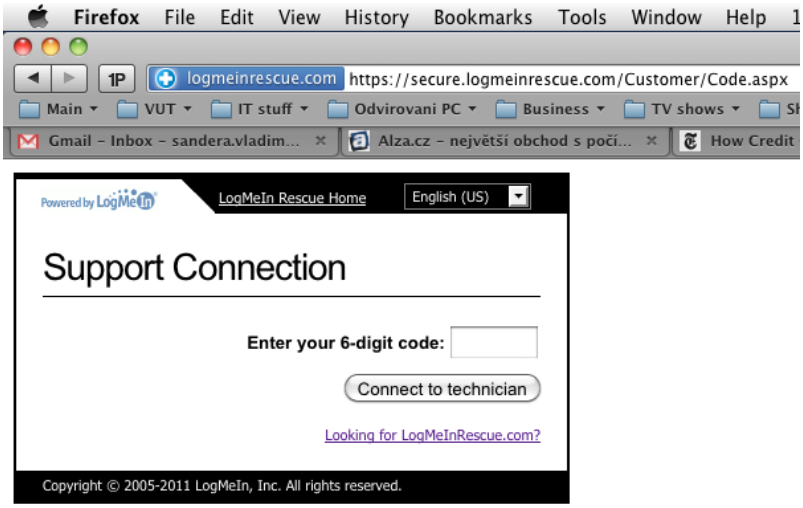
5.3.2 Úprava webových stránek

Pro zavedení nového modelu poskytování služeb online bylo třeba upravit webové stránky. Ponechali jsme stávající doménu odvirovanipc.cz. Nabídku služeb jsme upravili tak, aby zákazník při návštěvě webu pochopil, jak fungují nové služby. Do webových stránek byl zabudován odkaz na aplikaci LogMeIn pro okamžité vzdálené připojení. Průběh připojení k zákazníkovi přes naše stránky pomocí aplikace LogMeIn Rescue:



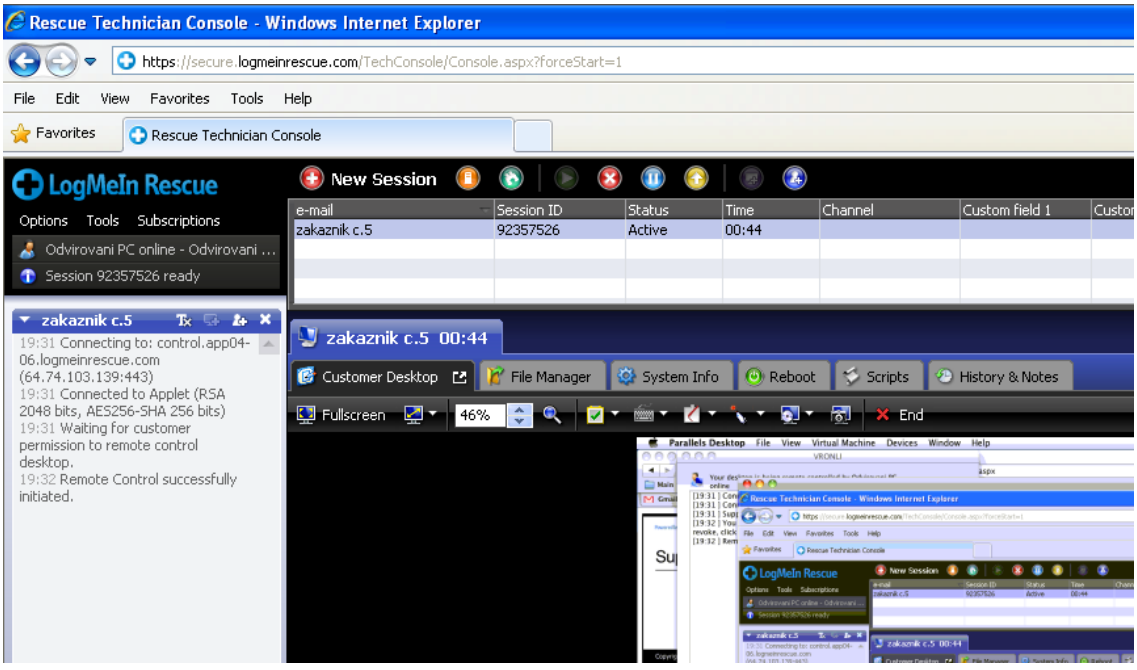
Obr. 10: Firemní webové stránky, zdroj: vlastní

1. Zákazník otevře internetové stránky www.odvirovanipc.cz a na základě instrukcí technika klikne na poptávanou službu, např. na "Odvirování PC na dálku". Nadpisy služeb slouží jako odkazy.



Obr. 11: Rozhraní pro vzdálené připojení, zdroj: https://secure.logmein.com/Customer

2. Zákazník je přesměrován na přihlašovací stránku aplikace LogMeIn, kde zadá 6-místný kód, který mu sdělí technik. Po zadání kódu je zákazník vyzván ke spuštění exe souboru aplikace. Po spuštění je ihned navázáno vzdálené spojení s technikem.



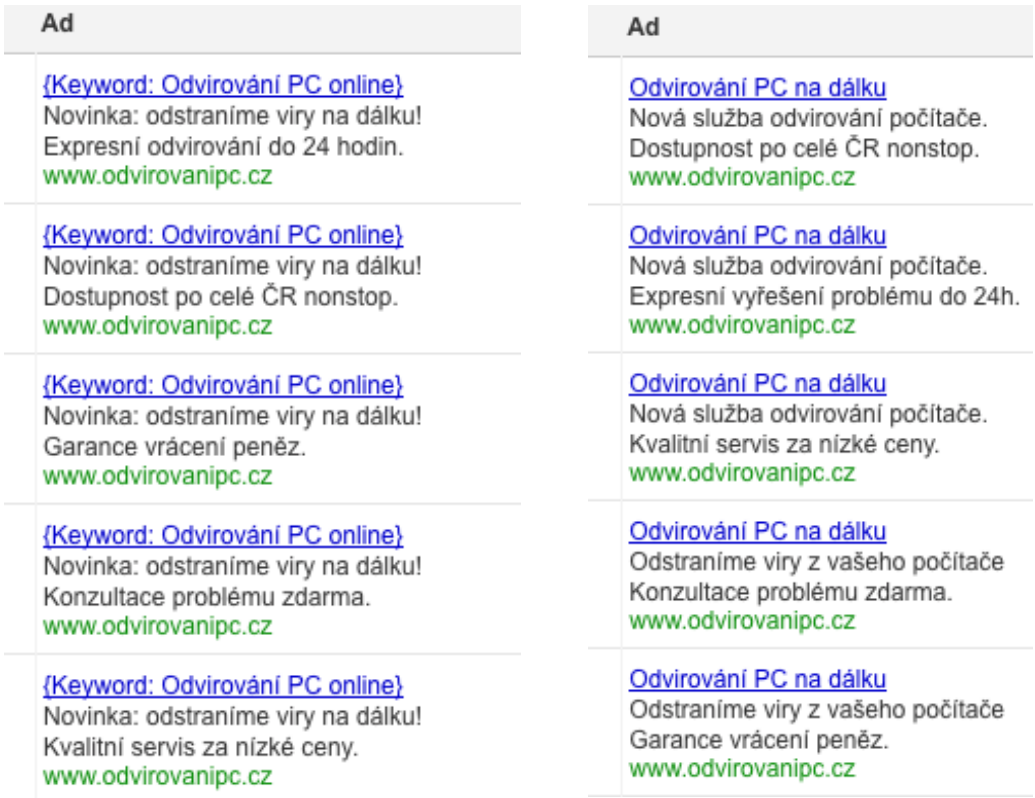
Obr. 12: Konzole LogMeIn, zdroj: z vlastních dat generováno https://secure.logmein.com/TechConsole

3. Nyní jsme připojeni k zákazníkovi. Toto je rozhraní LogMeIn konzole, které vidí technik. Přes rozhraní ovládáme vzdálené připojení. Vpravo dole je zobrazena vzdálená plocha počítače zákazníka. Celá aplikace běží v internetovém prohlížeči.

5.3.3 Úprava marketingových kampaní

Vzhledem k tomu, že provozuji téměř výhradně internetový marketing, je velmi jednoduché provést úpravy běžících kampaní. V nastavení PPC kampaní na vyhledávačích Seznam.cz a Google.cz jsem modifikoval cílení z okresu Brno-město a Brno-venkov na celou republiku.

Byly také provedeny úpravy reklamních textů, aby vystihovaly nový online model nabízených služeb. Zde uvádím dvě sestavy nově vytvořených reklamních textů:



Obr. 13: Reklamní texty pro PPC reklamu, zdroj: z vlastních dat generováno https://adwords.google.com

5.4 Podnikatelská strategie a cíle

5.4.1 Rozšíření služeb

Do budoucna plánuji kromě jednorázových služeb nabízet dlouhodobou technickou podporu i formou předplatného. Zákazník si za určitou částku objedná roční technickou podporu, zaplatí předem stanovenou částku a po dobu jednoho roku mne bude moci kontaktovat ohledně technických problémů a nebude již platit za jednotlivé zásahy. Typy služeb dále diferencuji. Kromě "odvirování PC na dálku", budou k dispozici i další služby jako servis PC na dálku nebo instalace aplikací na dálku.

Dlouhodobým cílem je vytvořit partnerství s antivirovými společnostmi a poskytovateli internetového připojení v ČR a outsourcovat část jejich technické podpory. V tomto případě adoptuji model, který se již začíná realizovat v USA. Typickým příkladem nezávislé společnosti poskytující online technickou podporu je support.com.

5.4.2 Vytvoření pracovního teamu

V nejbližší době se chystám do procesu zapojit a proškolit další studenty, kteří se postupem času stanou mými spolupracovníky. Mým cílem je vyškolit si team spolupracovníků, kteří budou provádět nabízené služby. Do dvou let plánuji zaměstnat 5 - 10 pracovníků. Garantovanou dostupnost služby bude od 8h do 24h, 7 dní v týdnu. Tento časový úsek se rozdělí na směny, na které budou přiděleni jednotliví pracovníci.

Pracovníci budou pracovat na zaměstnanecký poměr s měsíční mzdou 8 000 Kč, ke mzdě budou přičítány příplatky za úspěšné servisní zásahy. Každý zaměstnanec bude mít příplatek za každý úspěšně provedený servisní zásah. Výdělek pracovníka se tedy bude z velké části odvíjet od úspěšnosti jeho práce. Tento platební model bude motivovat zaměstnance k dosahování lepších výkonů.

5.5 SWOT analýza

Silné stránky	**Slabé stránky**
- cenová politika: nízké a fixní ceny, zákazník dopředu ví, kolik zaplatí - dostupnost: služba je poskytována 7 dní v týdnu s dostupností od 8h do 24h, v budoucnu je možné fungovat 24/7 - rychlost zásahu: okamžitá reakce na zákazníkův dotaz / problém - pokrytí celé ČR i zahraničí - pokročilá znalost i zkušenosti v oblasti zabezpečení PC - mladý kolektiv studentů – schopnost zůstat flexibilní a rychle se přizpůsobovat změnám prostředí	- nutnost interakce ze strany zákazníka, abychom se připojili na jeho PC. Pokud má zákazník nízké technické znalosti, může být tento proces zdlouhavý. - ne všechny problémy zákazníků jsou řešitelné vzdáleně. - pomalé internetové připojení způsobuje prodlužování doby zásahu - pokud počítačová infekce zablokuje spouštění exe souborů, není možné navázat připojení k zákazníkovi - obtížné školení pracovníků: vysoké nároky na technické znalosti pracovníků, rozsáhlá množina potencionálních problémů, na které můžeme u zákazníka narazit
Příležitosti	**Hrozby**
- rozrůstající se počet uživatelů internetu, tudíž i počet potencionálních zákazníků - technické problémy uživatelů jsou globální => jednoduchá expanze na zahraniční trhy - služba má potencionál změnit chování uživatelů PC. Namísto	- malé bariéry pro vstup na trh => do budoucna vznikne silná konkurence - s rozšířením online podpory začnou počítačové infekce blokovat aplikace pro vzdálené připojení - uživatelé začnou pro řešení

toho, aby problém řešili sami nebo přes přítele, se jim vyplatí využít našich služeb - rozšíření služby na mobilní segment: chytré telefony s operačním systémem jsou také náchylné k softwarovým problémům a infekcím - partnerství s prodejci počítačů => prodej online podpory společně s počítačem	problémů využívat anglicky psaná diskuzní fóra technické podpory a fóra typu Q&A, kde si najdou řešení problému zdarma.

6. Zhodnocení a závěr

Z důvodu obrovského potencionálu technické podpory online jsem se rozhodl kompletně přejít na nový model a nabízet služby zabezpečení PC na dálku. Dále jsem rozšířil svoje zaměření na další servisní služby, které se dají na dálku realizovat. Cílem mého podnikání je vybudovat nezávislou servisní společnost, která bude poskytovat placené online služby pro segment koncových uživatelů a malých firem.

Online segment technické podpory dle mého názoru postupem času ovládne celý trh technické podpory a vytlačí fyzické servisní zásahy, které se stanou minoritním segmentem na trhu. Tento trend vývoje je již patrný na americkém trhu a během následujících let dorazí i do České republiky. Počet uživatelů internetu na Českém trhu se stále zvyšuje a uživatelé ve stále větší míře využívají internet pro online bankovnictví a nakupování produktů. Se změnou chování spotřebitelů se zároveň zvyšuje důležitost zabezpečit počítač a zajistit rychlou technickou podporu v případě, že dojde k problému s počítačem nebo s používanými aplikacemi.

Masové rozšíření připojení uživatelů k internetu, které proběhlo v ČR během posledních 10 let, umožňuje v současné době efektivně nabízet technickou podporu na dálku bez nutnosti fyzického výjezdu technika k zákazníkovi. Poskytování služeb online zajisté přináší nová technická úskalí. Výhody online modelu ale jednoznačně převyšují negativa. Z mého pohledu jakožto podnikatele na trhu technické podpory je nezbytné nastartovat přechod na online služby co nejdříve. V České republice jsem byl prvním podnikatelským subjektem, který začal na internetu nabízet placenou technickou podporu online pro koncové zákazníky.

Seznam použité literatury

Knižní publikace

[1] DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. USA : McGraw-Hill, 2010. 377 s. ISBN 978-0-07-159118-8

[2] AYCOCK J. *Computer Viruses and Malware*. USA : Springer, 2010. 227 s. ISBN 978-0-387-30236-2

[3] JOHNSTON J. *Technological Turf Wars: A Case Study of the Computer Antivirus Industry.* USA : Temple University Press, 2008. 232 s. ISBN 978-1592138821

[4] SZÖR P. *The Art of Computer Virus Research and Defense*. USA : Addison Wesley Professional, 2005. 744 s. ISBN 0-321-30454-3

[5] JANOUCH V. *Internetový marketing Prosaďte se na webu a sociálních sítích.* 1. vydání. Brno : Computer Press, a.s., 2010. 304 s. ISBN 978-80-251-2795-7

Internetové zdroje

[6] ČSÚ. *Využívání ICT jednotlivci.* [online]. 2010 [2011-5-7]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/vyuzivani_ict_jednotlivci_2005_2010/$File/Vyu%C5%BE%C3%ADv%C3%A1n%C3%AD_ICT_jednotlivci_2005_2010.xls

[7] ČSÚ. *Počítačové dovednosti.* [online]. 2010 [2011-5-7]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/pocitacove_dovednosti/$File/3_pc_dovednosti_eu.xls

[8] ČSÚ. *Nákupy přes internet.* [online]. 2010 [2011-4-7]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/nakupy_pres_internet/$File/7_nakupy_pres_internet.xls

[9] IT-software.com. *Top 10 remote support software vendors.* [online]. 2011 [2011-4-21]. Dostupné z: http://www.business-software.com/it-management-solutions/remote-support/index.php

Seznam obrázků

Obr. 1: Návštěvnost webu, zdroj: z vlastních dat generováno https://www.google.com/analytics 14

Obr. 2: Daňová povinnost a zdravotní poj., zdroj: z vlastních dat generováno http://www.podnikatel.cz 15

Obr. 3: Analýza bodu zvratu, zdroj: z vlastních dat generováno http://www.calculatorplus.com 16

Obr. 4: Uživatelé s každodenním využitím internetu 20

Obr. 5: PC dovednosti uživatelů, zdroj: ČSÚ. *Počítačové dovednosti.* 2010. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/pocitacove_dovednosti/$File/3_pc_dovednosti_eu.xls 21

Obr. 6: Chování uživatelů – nákupy přes internet, zdroj: ČSÚ. *Nákupy přes internet*. 2010. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/nakupy_pres_internet/$File/7_nakupy_pres_internet.xls 21

Obr. 7: Architektura systému MS Windows, zdroj: DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. 2010. s. 125 32

Obr. 8: Virtualizace systémových zdrojů, zdroj: DAVIS M., BODMER S., LEMASTERS A. *Hacking Exposed Malware & Rootkits*. 2010. s. 175 34

Obr. 9: Firemní logo, zdroj: vlastní 44

Obr. 10: Firemní webové stránky, zdroj: vlastní 48

Obr. 11: Rozhraní pro vzdálené připojení, zdroj: https://secure.logmein.com/Customer 49

Obr. 12: Konzole LogMeIn, zdroj: z vlastních dat generováno https://secure.logmein.com/TechConsole 49

Obr. 13: Reklamní texty pro PPC reklamu, zdroj: z vlastních dat generováno https://adwords.google.com 50

Seznam grafů

Graf 1: Antivirové aplikace zákazníků, zdroj: vlastní 16

Graf 2: Problémy zákazníků, zdroj: vlastní 16